1.2502

ABSTRACT OF THE DISCLOSURE

SECURE NETWORK IDENTIFICATION

09930113

A processing unit is connectable to a data communications network. The processing unit includes a device reader for a portable storage device. The portable storage device (e.g., a secure smart card) includes storage operable to supply a network identity for the processing unit and an access controller. The access controller is operable to prevent unauthorised writing to the storage. Before reading the network identity from the portable storage device, the processing device attempts a write to the storage of the portable storage device, and, only on determining that the write has failed, reads the supplied network identity. The processing unit is thereby able to check that the portable storage device is a valid secure data storage device and not a counterfeit portable storage device. If it is a genuine secure portable storage device, the write access will not be permitted, whereas if it is a non-secure portable storage device, there is a risk that it is a counterfeit. The access control logic of the portable storage device can be operable to implement key-to-key encryption. The processing unit can be operable to modify the content of the storage of the portable storage device by supplying a key to the access controller, and, in response to receipt of a return key from the access controller, to send an encrypted command to modify the content of the storage of the portable storage device.

Fig. 9